



THE LEADER IN **SECURITY OPERATIONS**

# Warum so viele Organisationen leicht Opfer für Cyber-Kriminelle werden

Dr. Sebastian Schmerl

©2024 Arctic Wolf Networks, Inc. All rights reserved. Public

Stand 435  
Halle 7

# Agenda

- 01 General Threats**
- 02 Frequent Attacks in Detail**
- 03 Shiny Object Syndrome**
- 04 State of the Art Cyber Protection**



# 01

## General Cyber Threats

Really no major changes in the last year?



# Current Cyber Security Threats

Most of them are very hard to prevent, which makes them so successful



## Phishing likes News

GENERATIVE AI



## Leaked Passwords



## Remote Work Exploitation



## Zero-day exploits



## Business Email Compromise

GENERATIVE AI



## Deepfakes & Identity Theft

GENERATIVE AI



## Ransomware Attacks and Double Extortion



## Cloud Breaches / Takeovers

... to be continued



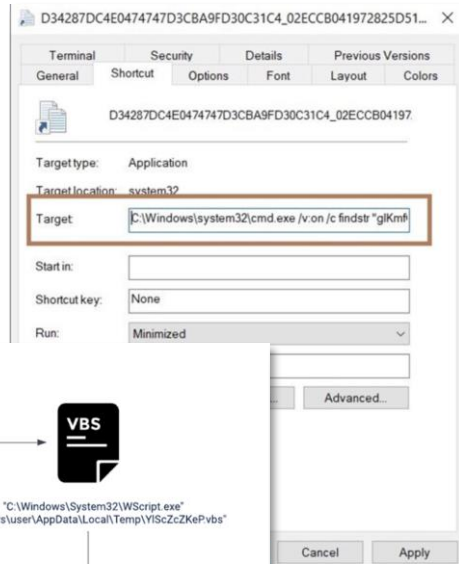
# 02

## Frequent Attacks in Detail

in the DACH Region

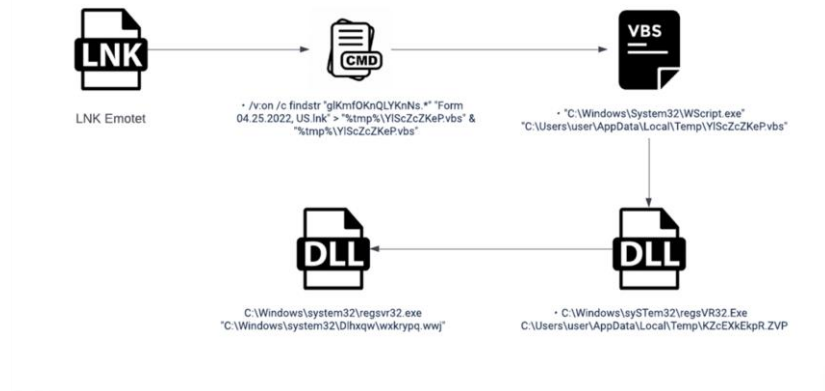
# Frequent Attack Types 1

Malicious files (.lnk .html .pdf .iso, ...) send as attachments



## Usage of User known Files/Icons

- Multi-Stage-Attack
- First Stage:
  - Phishing Email with attachment
  - .lnk files which extract script content
  - VBS, js, ps scripts
  - Download second stage from WWW



Monitoring &  
Detection



# Frequent Attack Types 2

## LOLBINs & LOLDRIVERSs



### Living on the Land via :

- LOLbins: Use installed software mainly for:
  - Downloading content
  - Execution of content/code
  - <https://lolbas-project.github.io/>
- LOLdrivers: Use installed drivers mainly for:
  - Bypass security controls
  - Execute content/code
  - <https://www.loldrivers.io/>

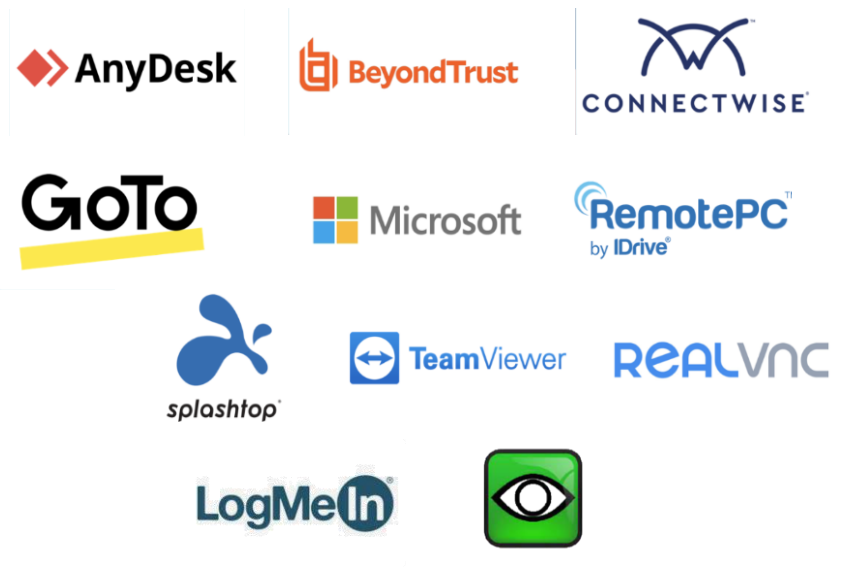


Monitoring & Detection



# Frequent Attack Types 3

## Usage of the organizations own Remote Access Tools



### Attackers are using legitimate Remote Access Software

- Download, install and persists
- Most AVs do not report these files
- Some attackers are doing reconnaissance for reusing the Remote Access Software installed on systems.



Monitoring &  
Detection





# Frequent Attack Types 4

## Token & Tickets & APIs



### Cloud API & Token exploitation

- API Usage via Token Authentication does not require for MFA
- Not secured APIs -> often seen on Webpages
- Tokens are often embedded in scripts and communicated in cleartext
- O365 Token – aka Golden <SAML/> Tickets



Monitoring &  
Detection

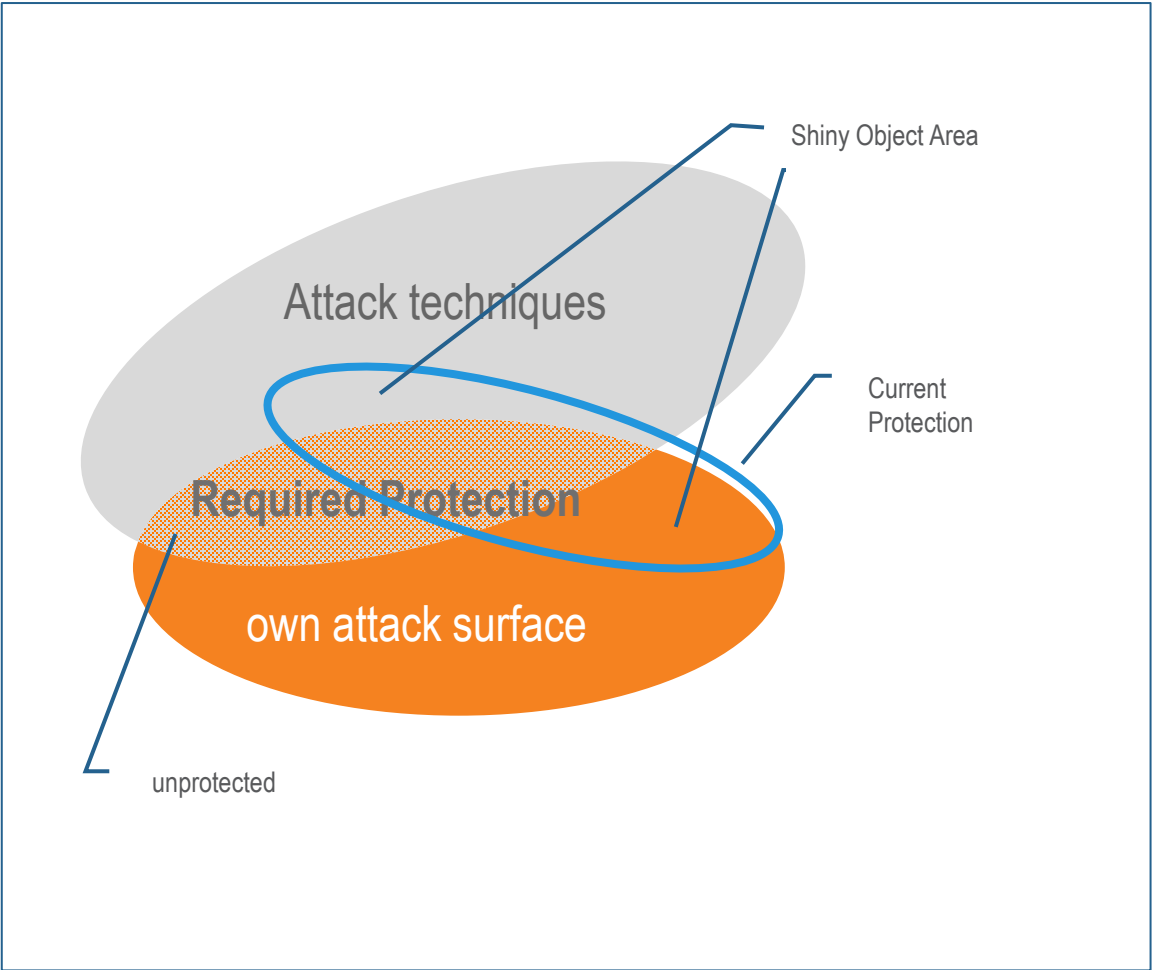








# 03

## Shiny Object Syndrome

# Shiny Object Syndrome

Adapting security to required scope and not vice versa



Shiny Object	Target Group	Result
		
  	<ul style="list-style-type: none"><li>• Board Level</li><li>• Peer Groups</li><li>• CISO</li><li>• IT</li></ul>	No alignment with required protection



# 04

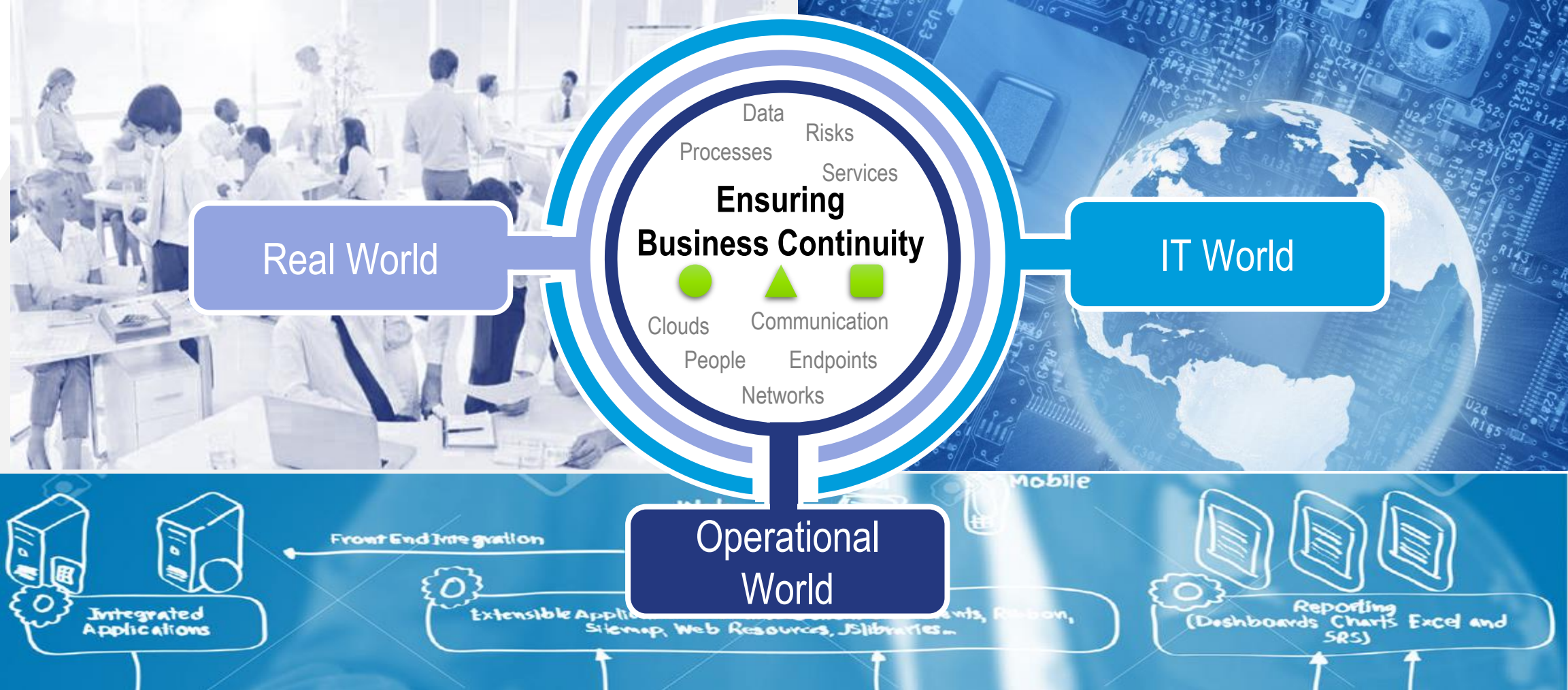
## State of the art Security Protection



# Cyber-Defense @ Arctic Wolf

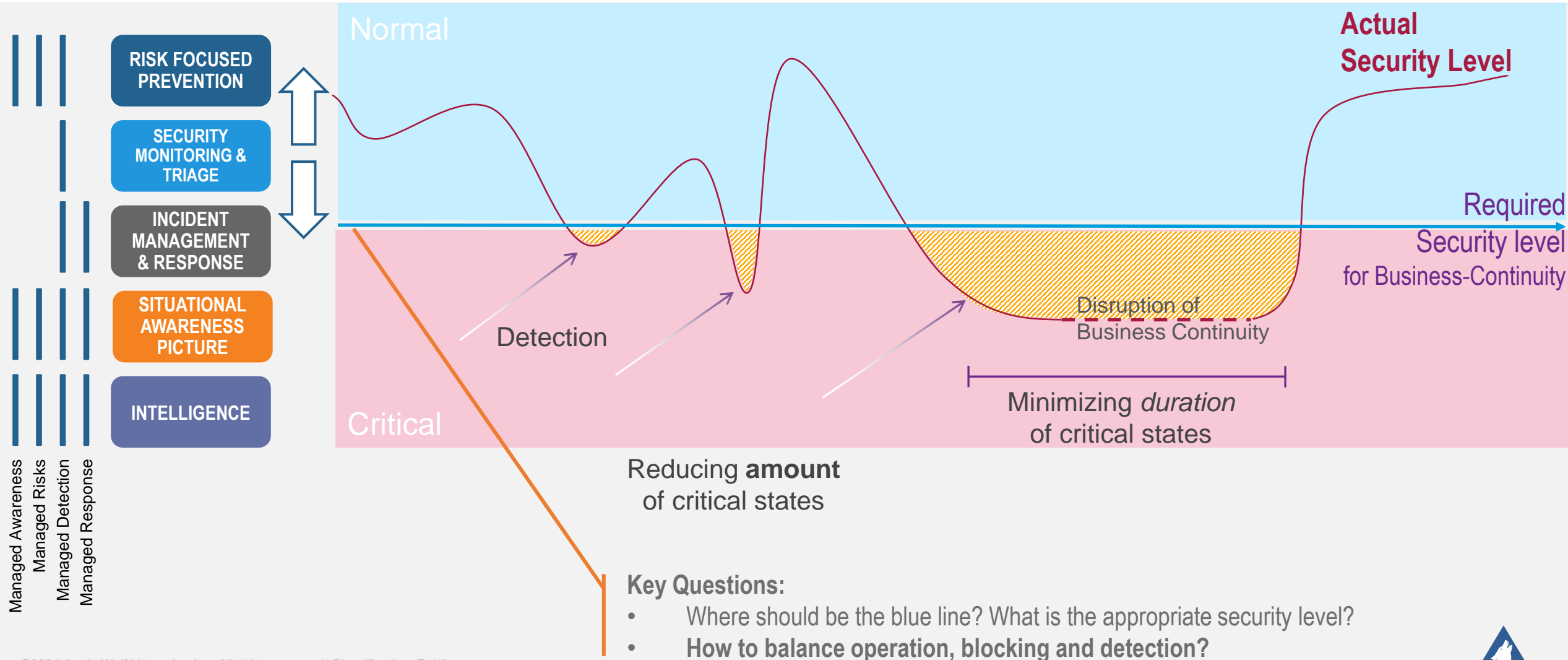
THE LEADER IN **SECURITY OPERATIONS**

## THREE WORLDS, THREE PERSPECTIVES, BUT ONE GOAL



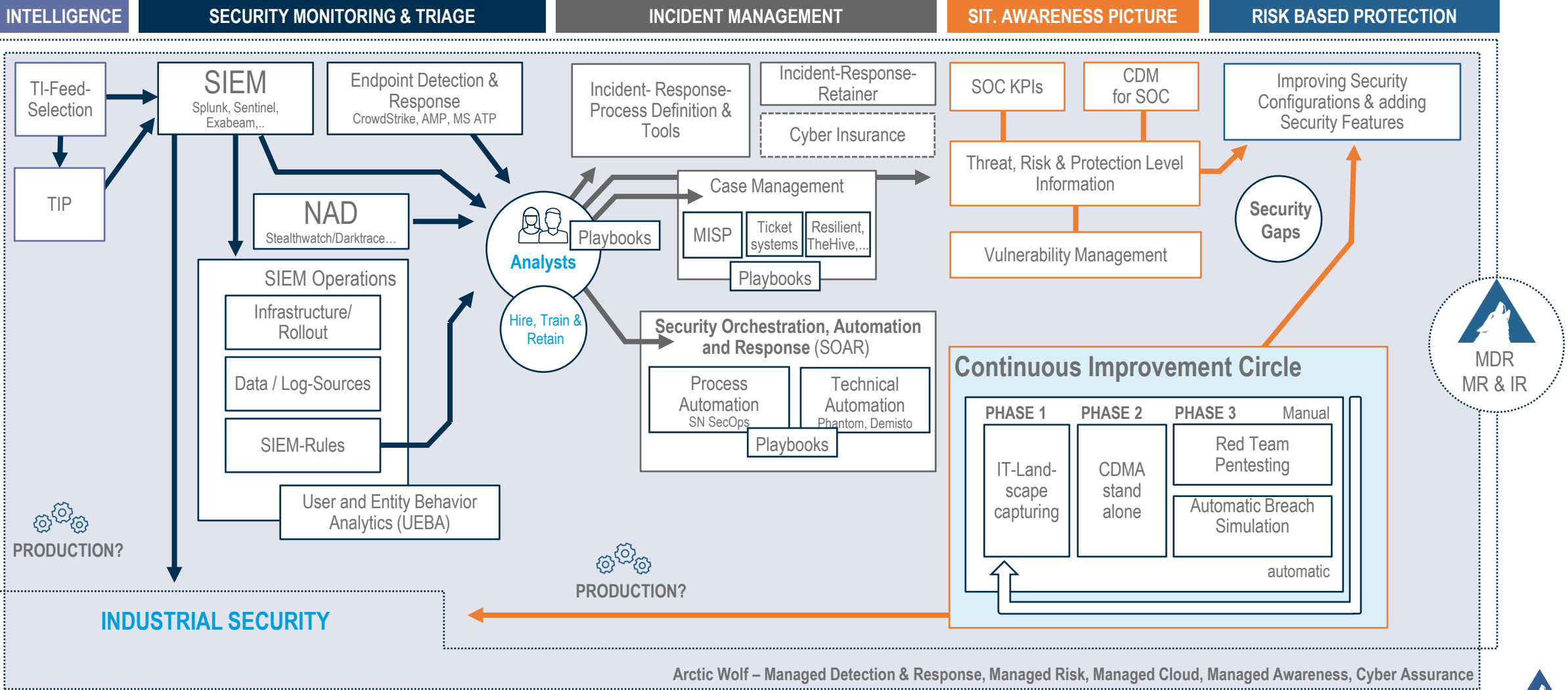
# General Cyber Defense Strategy

AWARENESS, PROTECTION, DETECTION, REACTION, RESILIENCE



# Cyber Protection – Building Blocks you need to cover

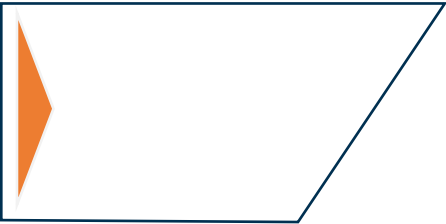
## STATE-OF-THE-ART CYBER DEFENCE



# Thank You

**SECURITY IS NOT A CHOICE  
IT IS A NECESSITY**

**ARCTIC WOLF: *IT'S TIME TO END CYBER RISK***







THE LEADER IN **SECURITY OPERATIONS**

# END CYBER RISKS

<https://arcticwolf.com/de/>  
<https://arcticwolf.com/de/security-operations-platform/>  
<https://arcticwolf.com/de/concierge-security/>